Developing a Comprehensive Information Security Framework for mHealth: A Detailed Analysis

Nattaruedee Vithanwattana
School of Science and Technology
Middlesex University,
Hendon, London NW4 4BT
Email: nv166@live.mdx.ac.uk

Glenford Mapp
School of Science and Technology
Middlesex University
London, UK
Email: g.mapp@mdx.ac.uk

Carlisle George
School of Science and Technology
Middlesex University
London, UK
Email: c.george@mdx.ac.uk

***Abstract*—It has been clearly shown thatmHealth solutions, which is the use of mobile devices and other wireless technology to provide healthcare services, deliver more patient-focused healthcare and improve the overall efficiency of healthcare systems. In addition, these solutions can potentially reduce the cost of providing healthcare in the context of the increasing demands of the ageing populations in advanced economies. These solutions can also play an important part in intelligent environments, facilitating real-time data collection and input to enable various functionalities. However, there are several challenges regarding the development of mHealth solutions: the most important of these being privacy and data security. Furthermore, the use of cloud computing is becoming an option for the healthcare sector to store healthcare data; but storing data in the cloud raises serious concerns. This paper investigates how data is managed both on mHealth devices as well as in the cloud. Firstly, a detailed analysis of the entire mHealth domain is undertaken to determine domain specific features and a taxonomy for mHealth, from which a set of security requirements are identified in order to develop a new information security framework. It then examines individual information security frameworks for mHealth devices and the cloud, noting similarities and differences. Furthermore, key mechanisms to implement the new framework are discussed and the new framework is then presented. Finally, the paper presents how the new frameworkcould be implemented in order to develop an Advanced Digital Medical Platform (ADIMEP).**

Keywords—mHealth, Information Security, Wearable devices, Cloud Computing, Security Framework, Security Requirements

1. INTRODUCTION

The use of mobile and wireless technologies in healthcare systems has an enormous potential to transform healthcare across the globe[1]. Mobile Health or mHealth covers "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" [2]. mHealth is a subset of eHealth, which makes use of information and communication technologies to support the healthcare service. mHealth solutions include the use of mobile devices, such as mobile phones, tablets and wireless infrastructures. These devices are used in collecting clinical health data, delivering healthcare information to patients, medical professionals, and researchers. They are also used for real-time monitoring of patient vital signs, such as heart rate, blood glucose level, blood pressure, body temperature, brain activities, and direct provision of care [3].

mHealth devices can also be an integral part of intelligent environments, e.g. a Smart Home, facilitating real-time data collection from sensors and input to other devices to support various functionalities. According to the European Commission, there are nearly 100,000 mHealth applications available for users to download across various platforms including Google Play, iTunes, Blackberry World, and Windows Marketplace. There are already 231 million downloads worldwide on the top 20 free sports, fitness, and health applications. The European Commission has also predicted that by 2017 there will be 3.4 billion people worldwide who own mobile phone and 50% of them will be using mHealth applications. Moreover, mHealth would be able to save a total of €99 billion on the annual amount spent on healthcare in the EU if its potential is fully unlocked [2].

mHealth has potentially enormous impacts on healthcare by addressing budgetary challenges of healthcare systems and the ageing population. It delivers more patient-focused healthcare and improves the efficiency of healthcare systems. Diseases such as heart-disease, dementia, diabetes and obesity are beginning to affect large sections of the population of many countries and therefore threaten to overwhelm their medication health provision. A new approach is therefore needed which brings together various technologies to monitor and manage these diseases within populations. mHealth solutions will be able to detect the early stages of chronic conditions through the use of self-assessment tools and remote diagnosis. mHealth provides sustainable healthcare through better planning of patients' treatment which, in turn, reduces the number of unnecessary consultations and allows maximum benefits to be gained from the guidance in treatment and medication from healthcare professionals. Moreover, mHealth solutions could empower patients by enabling them to play a more participative role in medication. mHealth solutions can

help patients take more responsibility for their health through us of devices which can detect and report their vital signs, as well as mobile applications that will help them to be more focused on their diet and medication [4].

Generally, mHealth offers effective solutions to tackle problems in healthcare. However, there are still various challenges regarding the development of mHealth solutions. The most common issues are data security, funding, a lack of good examples of the efficacy and cost effectiveness of mHealth in practice as well as the need for more high-quality research [5].

mHealth data is sensitive personal data as defined by EU/UK data protection legislation; it reveals the state of our health which we may not want to share with everyone. Therefore, the data on mobile devices need to be kept securely until it can be transferred to a storage facility. Increasingly, cloud facilities are being used to centrally store and process healthcare data. By combining mHealth solutions with cloud storage, it is possible to develop an Advanced Digital Medical Platform (ADIMEP) to meet these security challenges. This has the potential to reduce the cost of processing and storing the data. However, storing and processing sensitive data in the cloud introduces several security concerns[6].

Security difficulties are some of the key challenges in mHealth. They include dealing with those who have the right to access healthcare records, either patients or healthcare professionals, and ensuring that only applications or devices that have been approved will be able to access healthcare data [7]. It is also necessary to comply with data protection requirements and ethical guidelines (e.g. regarding privacy) that impact on the processing of healthcare data.. For example, a third party (outside the doctor-patient relationship) must receive permission from a patient in order to use his/her personal data before conducting future research in healthcare.

In the past, many software vendors of healthcare information and some healthcare providers adopted the philosophy of "making it work first, then thinking about the security later". However, rapid technological changes and new developments as well as legal requirements (e.g. the requirement to use privacy enhancing technologies under new data protection legislation) have made information security a priority to protect the confidentiality and privacy of healthcare information [8]. Various security methods should be enforced in order to secure mHealth information from the risk of unauthorised access. To ensure the security of mHealth data, the CIA triad which includes: Confidentiality (the assurance that data cannot be viewed by an unauthorised user): Integrity (the assurance that data has not been altered in an unauthorised manner); and Availability (the assurance that data will be available anytime when it is needed) should be applied to mHealth solutions.

Previously, there have been many attempts to build new information security frameworks. Some examples include: a detailed specification [9]; a comprehensive SecureCloud framework [10]; Cloud Security Framework (CSF) [11]; The user-specific security requirements for end clients [12]; and a security framework based on Capabilities [13]. However, there is no framework that has been shown to have the complete set of functions that are required for mHealth.

This paper is an extension of *"mHealth – Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions"* which was presented at *the 12th International Conference on Intelligent Environments (IE'16)*. The paper is structured as follows: Section 2 identifies the mHealth domain specific features and provides a taxonomy of the mHealth system which maps the entire structure of the mHealth system in order to develop it into an ontology of an mHealth system. The section also includes a discussion on the management of mHealth data on mobile devices and in cloud storage. Further an analysis of existing information security frameworks for mHealth devices and the cloud is given, and challenges in managing mHealth data are identified; Section 3, discusses the key mechanisms to implement the new information security framework for managing healthcare data in the mHealth system. In Section 4, a new information security framework for cloud-based infrastructure is proposed based on the use of key mechanisms discussed in Section 3. In Section 5, an Advanced Digital Medical Platform (ADIMEP) is presented as a new approach to tackle the challenges of large-scale diseases. Section 6 represents the future work plan in developing an mHealth ontology and building ADIMEP. The paper concludes in Section 7.

2. MHEALTH DOMAIN SPECIFIC ANALYSIS

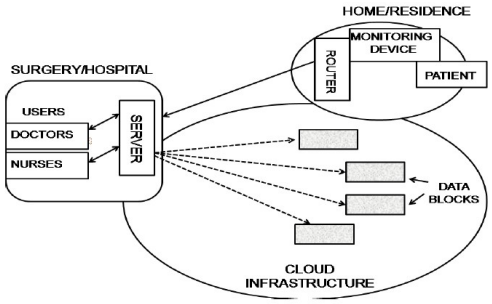

Figure 1: mHealth system scenario

In mHealth systems, healthcare data will be collected from mHealth devices such as wearable devices or implanted devices. The collected healthcare data are generally transferred via Bluetooth or Zigbee to mobile phones/tablets/ PDAs, which mHealth applications installed on them. The healthcare data will be stored on mobile devices until the data can be transferred over the network to healthcare professionals' servers and then stored in the cloud. The scenario is shown in Figure 1. Therefore, healthcare professionals will be able to access their patients' healthcare data through cloud storage without the need for a physical meeting between the healthcare professionals and patients.

2.1 DEVELOPING TAXONOMY OF MHEALTH SYSTEM

Taxonomies have been used in many fields for a long time. For example, in botany, a taxonomy has been used to classify plants. A taxonomy is the basis of classification schemes and indexing systems in information management [14]. A taxonomy is usually a hierarchy of concepts which only shows the relationship between each concept such as parent and child, or superclass and subclass. One purpose of a taxonomy is to give a knowledge representation of a classification. A taxonomy is related to a similar but more complex concept called an ontology. An ontology goes beyond knowledge representation. An ontology represents the conceptualization of a domain in a system. It defines **classes** (sometimes called **concepts**) that describe concepts of the domain, **subclasses** that represent concepts that are more specific than the

superclass, **slots** (sometimes called **roles** or **properties**) which describe properties of classes and instances, and **facets** (sometimes called **role restrictions**) which describe the restrictions on slots. In order to develop an ontology, all classes in the ontology need to be defined and arranged into a taxonomic (subclass-superclass) hierarchy. Slots will also be defined and allowed values for these slots are described, as well as filling in the values for slots [15].

Cloud computing provides several types of services, including virtualized storage and development platforms. Therefore, the complexity of cloud computing leads to the development of different dimensions of taxonomy which aims to classify the different type of services as well as group those with similar characteristics [16].

One of the most well-accepted cloud computing taxonomies is NIST's SPI Model (Figure 2) [17]. The main objective of this taxonomy is to encompass various service models of cloud computing. The SPI model comprises three categories [17]:

- *Software as a Service (SaaS)* – The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- *Platform as a Service (PaaS)* – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
- *Infrastructure as a Service (IaaS)* – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

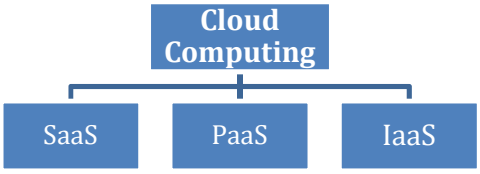

Figure 2: The NIST's SPI Model [18]

Judging that NIST's SPI model was oversimplified [16], Johnston (2010) [18] developed a cloud computing taxonomy which organizes the cloud ecosystem in six layers (Figure 3) detailed as follows [18]:

- *Clients*: Computer hardware and/or computer software which rely on the cloud to deliver services and applications
- *Services*: Software systems designed to support interoperable machine-to-machine interaction over a network
- *Application*: Solutions which eliminate the need of installing or running software on local machines [16]
- *Platform*: Computing platform facilitates deployment of applications without the complexity and the cost of purchasing the required infrastructure.
- *Storage*: The delivery of data storage as a service
- *Infrastructure*: The delivery of computer infrastructure as a service.

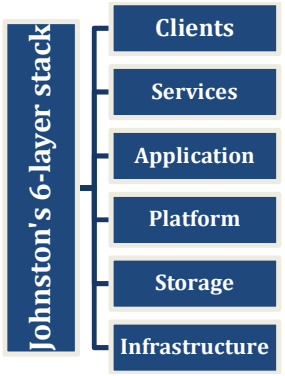

Figure 3: Johnston's 6-layer stack [18]

Previously, there have been some developments of taxonomy for mobile devices and cloud computing which are key components of mHealth systems. However, there is no taxonomy that encompasses mobile devices and cloud computing in order to address a complete set of mHealth system concepts/components including system architecture, data transmission in the system, stakeholders who interact with data in the system and, importantly, security requirements that should be proposed in order to secure data in the mHealth system.

Figure 4 shows a taxonomy of an mHealth system developed by that authors. In order to develop this taxonomy, a domain analysis of the mHealth system was carried out. The structure of the mHealth system was categorized into several components, including system architecture, healthcare data, stakeholder, and security requirements.

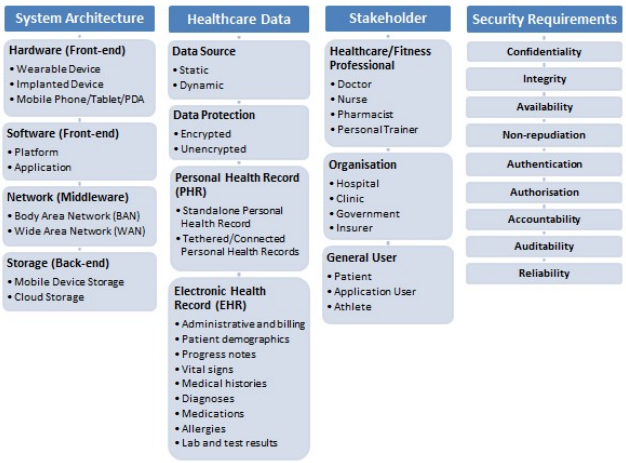

Figure 4: mHealth Taxonomy

1) *System Architecture*

The first-level taxonomy of the mHealth system is based on the architecture of the mHealth system. This can be defined in terms of Front-end (Hardware and Software), Middleware (Network), and Back-end (Storage).

A.Hardware can be defined as the physical components (or mHealth devices) in mHealth systems. Hardware in mHealth systems consist of:

- *Wearable Devices:* Wearables refer to hand-held health electronic devices that are mounted on a user's body interface. They can perform many computing tasks that are not typically seen in mobile and laptop devices including sensory and scanning features. Some

wearable devices such as Fitness-tracking bands (e.g. Fitbit, Jawbone, Runtastic) are good examples of the Internet of Things. Some other examples of wearable devices include Smartwatches (e.g. Android Wear, Apple Watch, Pebble Watch), and Smart Glasses (e.g. Google Glass, Sony's SmartEyeGlass)

- *Implanted Devices:* An implant is a medical device manufactured with the intention of replacing a missing body structure, supporting a damaged body structure, or enhancing an existing body structure. An implanted device can be placed permanently or can also be removed once it is no longer needed [19]. Examples of implanted devices include: an artificial heart, neurostimulator, and Circadia (Human Embedded Light Emitting Diode Display (HELEDD)) [20].
- *Mobile Phone/Tablet/Personal Digital Assistant (PDA):*These devices are used to perform a variety of information management functions in mHealth systems. An authorised mHealth application will be installed on a mobile phone, PDA, or tablet in order to communicate with wearable devices and implanted devices embedded on a user's body. Wearable devices and implanted devices collect healthcare data from the user and transfer it to a mobile phone/tablet/PDA. Healthcare data may be collected in these devices' databases or will be transferred to be stored in cloud storage.

B. Software can be defined as the various kinds of computer programs operated by mHealth devices which are used to manage healthcare data in mHealth systems.

- *Platform:* In mHealth systems, a platform generally refers to a mobile operating system which is an operating system for mobile devices such as mobile phones, tablets, and personal digital assistants (PDAs). Current mobile platforms include: Android, iOS, Windows 10 Mobile, Ubuntu Touch OS, etc.
- *Application:* Software applications are designed to run on mobile devices. mHealth applications include the use of mobile devices in collecting healthcare data from users. Different mHealth applications may be designed to operate on different mobile platforms.

C. Network is defined as wired or wireless connections for the purpose of transmitting, receiving, and exchanging healthcare data in an mHealth system.

- *Body Area Network (BAN):*or sometimes referred to as *Wireless Body Area Network (WBAN) or Body Sensor Network (BSN)*is a communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics, personal entertainment, and others [21]. A BAN is characterised as an easily configured, low-cost, low-power, and highly reliable sensor system. The radius of operation of a BAN is just over a few feet. Healthcare data is generally transferred within a BAN via Bluetooth and ZigBee. Bluetooth is a developed technology that is widely used in many mobile phones, tablets, and PDAs. It allows communication bandwidth speeds of up to 720 kbps which is more than adequate for most body sensors. ZigBee is an emerging wireless standard for low-data rates, ultralow-power usage with a potential for use in mHealth systems. The maximum data rate of ZigBee is 250 kbps which is still sufficient for wearable devices and implanted devices [22].
- *Wide Area Network (WAN):*AWAN is a network that connects mHealth devices, data storage, and stakeholders in mHealth system across geographic regions such as towns, counties, or countries. The healthcare data communications which are established between a BAN and the remote terminals will be achieved by using WAN technologies such as 4G LTE, SSL VPN, or Fibre Optic.

D. Storage is where healthcare data in mHealth systems has been stored. Healthcare data could be stored using either *mobile device storage* or *cloud storage*. Healthcare data that is stored in cloud storage will be able to be accessed by stakeholders including healthcare professionals, organisations, or general users. However, information security is still the main challenge of mHealth systems because only authorised users should be granted access to healthcare data.

2) Healthcare Data

In mHealth systems, healthcare data refers to data that is stored and transmitted inthese system. The healthcare data is categorized by the source of data, presence of data protection mechanism, Personal Health Record (PHR) and Electronic Health Record (EHR).

A.Data Source can be categorized into two main types namely:

- *Static:* Once static data has been created, its content does not change over time. If it is changed, the data that has been changed will be considered as stateless, or no longer existing, and will be replaced by a new set of data. Examples of static data in mHealth systems include medical histories, allergies, and lab and test results.
- *Dynamic:* Dynamic data refers to the data that is asynchronously changed over time because there are new further updates becoming available. Vital signs (e.g. heart rate, body temperature, blood pressure) are good examples of dynamic data in mHealth systems.

B.Data Protection

- *Encrypted:*Strong encryption is the most effective way to achieve data security. Encrypted data refers to data that has been transformed into another form, so that only authorised parties who have a secret key will be able to gain access to it.
- *Unencrypted:*Healthcare data stored without any protections, and directly accessible.

C.Personal Health Record (PHR) is an electronic application used by patients to maintain and manage their health information in a private, secure, and confidential environment [23]. PHRs can contain healthcare information from various sources including healthcare professionals and patients themselves. PHRs can be categorised into two main types:

- *Standalone Personal Health Record:* The healthcare data in Standalone PHR is normally managed by a patient. Healthcare data may be stored either in mobile

device storage or in cloud storage. In some cases, a standalone PHR is able to be managed by external sources such as healthcare providers or laboratories. Patients can update their own healthcare data to track progress over time. Patients will be able to share their healthcare data with family members, healthcare professionals or personal trainers [23].

- *Tethered/Connected Personal Health Record:* A tethered/connected PHR is linked to an electronic health record (EHR) that is provided by a healthcare organisation. By using a tethered PHR, patients will be able to access their own healthcare record such as lab test results, medication histories, or diagnoses through a secure portal [23].

D.Electronic Health Record (EHR) is a digital record of healthcare information. EHRs are created to share healthcare data among healthcare professionals such as doctors, pharmacists, or laboratories. Only authorised parties, sometimes including the patients themselves, can access the data in an EHR. The difference between a PHR and an EHR is that a PHR is mainly managed by a patient, while an EHR is mainly managed by healthcare providers. The information in an EHR include: administrative and billing data, patient demographics, progress notes, vital signs, medical histories, diagnoses, medications, allergies, lab and test results. [24].

3) *Stakeholder*

In mHealth systems, stakeholders refer to authorised parties who have the right to gain access to healthcare data that are stored. There are three main stakeholders in mHealth systems.

A.Healthcare/Fitness Professionals: These are people who provide healthcare and well-being guidelines to general users. Healthcare/Fitness Professionals include: doctors, nurses, pharmacists, laboratory technicians, personal trainers, etc.

B.Organisations: Authorised organisations who are involved in the provisional of healthcare. They include: hospitals, clinics, laboratories, governments and insurers.

C.General users: mHealth device users who receive healthcare services from healthcare/fitness professionals. They include: patients, mHealth application users, and athletes.

4) *Security Requirements*

Security requirements describe the functional and non-functional requirements that need to be achieved in order to accomplish the security attributes of an mHealth system.From the threat analysis of mHealth systems (shown in Table 1) and previous research by Yahya, Walters, and Wills [25], the security requirements that are vital in order to protect the security of mHealth systems can be identified as follows:

A.Confidentiality: The assurance that data cannot be viewed by an unauthorised user [26]. Confidentiality is a common security component that is required in any security system. Healthcare data is classed as sensitive personal data under data protection legislation and the owner may not want to share his data with anyone. Therefore, only authorised parties will be able to access stored healthcare data.

B.Integrity: A key aspect of Information Security is Integrity. Integrity is the assurance that data has not been altered (which includes accidental alteration) in an unauthorised manner [26]. It is essential that an mHealth system should be able to detect if there are any deletions, modifications, or fabrications of healthcare data occurring in the system.

C.Availability: The assurance that healthcare data will be available and accessible to all authorised users every time it is needed [25]. System availability also includes the system's ability to carry on operations even when some parties misbehave. The system must have an ability to continue operations even when there is a possibility of security breaches [12].

D.Non-repudiation: The assurance that an entity cannot deny a previous commitment or action [26]. Non-repudiation is a strong requirement in mHealth systems since it requires the assurance that the original source of data cannot deny actions that have been conducted. However, most devices in mHealth systems do not support non-repudiation. The common methods of asserting non-repudiation are through public key encryption or digital certificates, and it is too expensive to apply these methods in mHealth devices. As a result, an alternative method needs to be proposed.

E.Authentication: Authentication is the process or action of verifying the identity of a user or process.In order to identify legitimate nodes between mHealth devices in mHealth systems, there is a process required to identify whether the received data is coming from authentic nodes [27]. Some processes include using passwords and biometrics (e.g. fingerprint, retina scan, voice recognition) to identify the user in order to gain access to mHealth devices. There are numerous types of security mechanisms such as digital signatures, digital certificates, or public key encryption that can provide the authentication process before transmitting healthcare data [27].

F.Authorization: Authorization is a process by which a system determines the security level for access or using resources within the system by each user. Whereas authentication is the process of identifying legitimate nodes or users within a mHealth system, authorisation is required to allow users such as patients or healthcare professionals to access stored healthcare data to populate information required [27]. For example, patients sometimes may be allowed to gain access to their own Electronic Health Record (EHR) but only authorised healthcare professionals are allowed to modify healthcare data in the EHR.

G.Accountability: Accountability is the process of keeping track of users' activity while accessing resources in the system. Accounting simply tracks which users accessed the mHealth system, what they were granted access to, the amount of data transferred during the session, the amount of time users spent on the system, and when they disconnected from the system [28].

H.Auditability: Auditability is highlighted as an important security component in mHealth systems. Therefore, it is important that each organisation in an mHealth system should perform routine security audits in order to ensure that healthcare data is protected as well as provides policies to comply with international IT standards [25].

I.Reliability: Reliability refers to the ability of a system to provide a consistent intended service most of the time [25]. According to the work of Mapp et al. [13], a security framework using capabilities could be used in mHealth systems to provide operational reliability.

2.2 SECURITY CHALLENGES IN MANAGING MHEALTH DATA

According to ISO27005, a threat is a potential cause of an incident that may result in harm to the system. Threats may be of natural or human origin and could be accidental or deliberate [29].

In mHealth systems, assets that require the protection, include mobile devices, cloud storage, connectivity, and healthcare data. This analysis will focus on where healthcare data is stored in mHealth systems, i.e., mobile devices and cloud storage.

a) Mobile device security threats

Mobile devices face a number of threats that may pose a significant harm to data which they store. The key mobile device security threats are identified as follows:

MT1. Loss and stolen: By the nature of mobile devices, they are prone to being lost or stolen. As a result, the users have a high risk of losing data stored on mobile devices.

MT2.Mobile malware: Mobile devices are vulnerable to malwares such as viruses, worms, trojans, spyware, ransomware, etc. Mobile malware are usually hidden inside some malicious mobile applications that users install or are deceived to install. Malware can disrupt mobile operations, gain access to sensitive personal data, or track user's activities.

MT3.Unauthorised access: Users normally store their login credentials for applications on their mobile devices. In this way, malicious attackers can easily access user's sensitive data in email and social network accounts.

MT4.Unlicensed and unmanaged software: The mobile software must be licensed and are required to be updated regularly. Failure of action could lead to unauthorized access to data or a significant loss of data.

MT5.Security of Biometrics: While a biometric system can enhance user convenience and strengthen the security of the system, it is also vulnerable to various types of threats as identified below [30]:

- Attacker is able to present fake biometric data presented to the sensor using prosthetic fingers created out of latex.
- Attacker modifies his own behavior (e.g.voice) to impersonate a weak biometric template.
- Attacker exploits a residual biometric image left on the sensor to impersonate the last authorized user.
- Attacker modifies (adding/replacing) biometric templates from storage.
- Attacker steals the biometric template database.

b) Cloud computing security threats

According to the Treacherous 12 Cloud Computing Top Threats [31], the repost identifies some key threats that may exploit the security of cloud computing as below:

CT1.Data breaches: Sensitive data is released, accessed, stolen or used by an unauthorized user.

CT2.Insufficient identity, credential and access management: The failure to use multifactor authentication, weak password, and poor key or certificate can lead to breaches and other attacks to cloud storage.

CT3.*Insecure interfaces and APIs*: The security and availability of cloud services is dependent on the security of user interfaces (UIs) and application programming interfaces (APIs). UIs and APIs are generally the most exposed part of the system and will be the target of heavy attacks.

CT4.System vulnerabilities: The attackers can use system vulnerabilities, or exploitable bugs, to penetrate a system for the purpose of stealing data, taking control of the system or disrupting service operations.

CT5.Account hijacking: If an attacker gains access to an individual's credentials, they can eavesdrop on the individual's activities, manipulate data, return falsified information and redirect the individual's clients to illegitimate sites.

CT6.Malicious insiders: Insider threats could be from any stakeholders who have authorized access to the system, network or data with an intention to exceed or misused that access in a manner that negatively affects the confidentiality, integrity or availability of data in the system.

CT7.Advanced persistent threats (APTs) are the parasitical forms of attack. APTs will penetrate the system to create a foothold in the computing infrastructure so that they can smuggle data and intellectual property over an extended period of time.

CT8.Data loss: Data stored in the cloud can be lost not only by deliberate actions but also by accident, such as an accidental deletion by the cloud service provider or a physical catastrophe including fire or earthquake. This can cause the permanently loss of data unless the provider or cloud consumer takes adequate measures to back up data.

CT9.Insufficient due diligence: Choosing cloud service providers without performing due diligence may lead to a myriad of commercial, technical, financial, legal and compliance risks that jeopardize success.

CT10.Abuse and nefarious use of cloud services: Poorly secured cloud service deployments expose cloud computing models to malicious attack. Some example of misuse of cloud service-based resources include launching DDoS attacks, email spam, phishing campaigns and hosting of malicious or pirated content.

CT11.Denial of Service (DoS): Attacks that are meant to prevent users from being able to access their data or their applications.

CT12.Shared technology issues: Cloud service providers deliver their services scalable by sharing infrastructure, platforms or applications. As a result, some users might be able to gain access to other user's actual or residual data and network traffic.

Table 1 represents an mHealth system threat list in which each threat is associated with the security requirements, C-Confidentiality, I-Integrity, and A-Availability, which are the fundamental parts of any security system.

Information Security / Threats	C	I	A
MT1	x	x	x
MT2	x	x	x
MT3	x	x	x
MT4	x	x	x
MT5	x	x	x
CT1	x	x	x
CT2	x	x	x
CT3	x	x	x
CT4	x	x	x

CT5	x	x	x
CT6	x	x	x
CT7	x	x	x
CT8			x
CT9	x	x	x
CT10	x	x	x
CT11			x
CT12	x	x	

Table 1: mHealth System Threat Analysis

Most threats that occur in mHealth systems have a significant potential to exploit confidentiality, integrity and availability which are the most common security requirements for mHealth systems. Therefore, developing security frameworks that can provide all mentioned security services is an essential part of managing data in mHealth system.

2.3 MANAGING mHEALTH DATA

mHealth systems generally store a large quantity of healthcare information such as the personal data of users, medical information, or symptom descriptions. Cloud computing also plays an important role in mHealth solutions as seen in Figure 5:

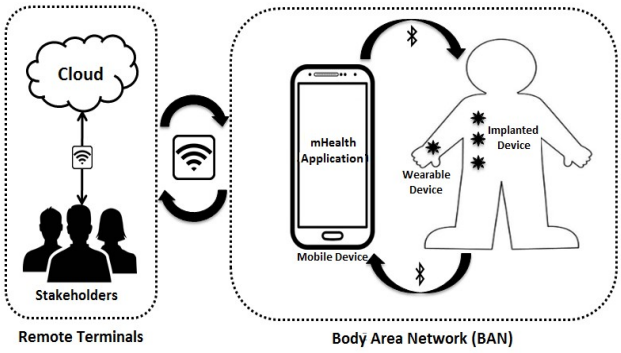

Figure 5: Managing mHealth data

In mHealth systems, mHealth devices which may be embedded or implanted inside the user's body or mounted to a user's body interface in a fixed position will collect healthcare data from the user using Bluetooth communication within a Body Area Network (BAN). Collected healthcare data will be transferred to remote terminals via a Wide Area Network (WAN) and will be stored in different databases including a mobile device's database and cloud storage. Authorised users, including healthcare professionals, patients, and mHealth users, will be able to access healthcare data in cloud storage using the Internet.

Cloud computing also plays an important role in mHealth systems. The main benefits of using cloud computing are that it provides an opportunity for end users to process large quantities of mHealth data in the cloud and supports a real-time, 24-7 data collection service. However, the information security of mHealth data is still the main challenge of managing mHealth data. Only authorised users should be able to access mHealth data in the cloud. Therefore, an appropriate information security framework must be applied to both mHealth devices and the cloud in order to secure the confidentiality of mHealth data from unauthorised parties.

1) Managing mHealth Data on Mobile Devices

The extensive usage of mobile phones, tablets and other mobile devices is an emerging phenomenon in the context of healthcare. Mobile devices are becoming a vital element for exchanging electronic healthcare data. Mobile devices also provide a significant advantage by allowing users to get Internet access from anywhere and at any time. However, some public wireless networks are usually unencrypted. As a result, a mobile device might become a vulnerable target to malware and other threats on the network.

However, the nature of mobile devices means that they are more likely to be lost or stolen. This may lead to the risk of lost or leakage of data that has been stored on the device. According to Christopher Paidhrin, (IT security compliance officer at Peace Health Southwest Medical Center in Vancouver, Washington, USA), "The inevitable loss of the device and, more costly, the loss of the data on the device is what's driving mobile security priorities" [32].

a) Mobile Data Collection System

A Mobile Data Collection System (MDCS) allow the collection and transmission of data from remote geographical locations to centrally located data storage repositories through wireless or cellular networks [33]. The mobile devices such as smartphones, tablets, or PDAs apply a MDCS in the system in order to gather information. `A MDCS requires two-way communication including immediate or delayed synchronization of data [34]. A MDCS consists of a few basic components as below:

1. Data Collection: Mobile devices are used in the process of data collection. This process could be either manually coded SMS forms (RapidSMS, FrontlineSMS, and Souktel AidLink) or by using a client application running on a mobile device. However, the SMS coded form-based data collection method does not handle complex forms and lacks skip logic and validation techniques. Therefore, more complex forms have been proposed in order to provide higher security. These include:

- **Native apps:** They are specific to a given mobile platform (Android, iOS, BlackBerry or Windows Mobile) using the development tools and languages that the respective platform supports (e.g. Objective-C with iOS, Java or C with Android, J2ME with Windows Mobile or BlackBerry). Native apps generally look and perform the best [33].
- **Web/HTML5:** Use of standard web technologies – typically HTML5, JavaScript and CSS. This write-once-run-anywhere approach to mobile development creates cross-platform mobile applications that work on multiple devices [33].
- **Hybrid apps:** They make it possible to embed HTML5 apps inside a thin native container, combining the best (and worst) elements of native and HTML5 apps [33].

2. Form Designer (Administrator Interface): It is used to create an electronic form from scratch or used to convert a traditional paper-based form into an electronic form. The mobile application has been designed in this process. It sometimes allows for data entry and viewing of the collected data. The administrator interface acts as the analysis platform and generally provides basic descriptive statistical functions as well as line graphs and bar charts [34].

3. Data Management: MDCS uses a centrally located server for managing, distributing form definitions and aggregating collected data [34]. Once data has been collected, the server will represent the data via the administrator client interfaces.

MDCS Data Flow

Figure 6 illustrates the data flow in a MDCS.

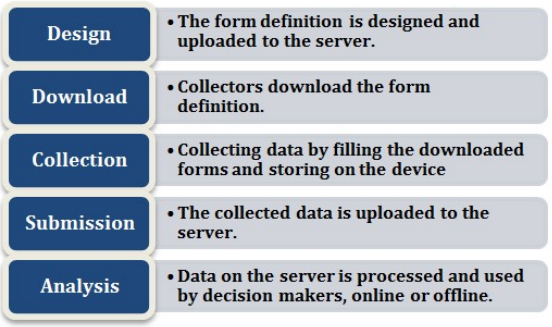

Figure 6: MDCS Data Flow

In relation to Figure 6 above, the form definition designs a form which consists of a set of questions for collecting and storing the relevant data in an accessible server database. Therefore, the collectors will be able to download these forms on their mobile devices and use them to collect actual data in the field. Each form that has been filled is stored on the mobile device until it is possible to upload (submit) the form to the central server where it will be stored and used for analysis [33].

b) MDCS Security Aspects

According to Gejibo (2015), he identified the different security aspects of MDCS based on the OWASP (Open Web Application Security Project) Top Ten Mobile Risks as below [35]:

1. Insecure Data Storage: Because of their small size, mobile devices are more prone to be lost or stolen. Some mobile devices provide a memory card slot which allows users to expand mobile storage with a memory card. Also,some of the application data on the mobile device is storedon the memory card without any protection mechanism being applied. In the case that mobile devices are lost or stolen, it may be easy for a thief or attacker to remove the memory card which contains data and read it on another mobile device. Moreover, a thief or attacker can also directly gain access to unencrypted data in mobile storage while the mobile device is on. As a result, it is necessary to encrypt the data before storing it on mobile devices.

However, there are also other unavoidable difficulties that accompany the encryption of data. For example, an attacker could possibly perform a cold boot attack, which is a type of side channel attack when an attacker can have physical access to a mobile device and obtains its encryption key. According to research from Princeton University (2008)[36], data that is stored in Dynamic Random Access Memory (DRAM) will be preserved for a brief period of time after a mobile device loses power. Cooling the memory, by keeping it at low temperatures or spraying with an inverted can of compressed air, can increase this period of time possibly up to hours. As a result, an attacker could gain access to data that remain readable in the period of time after power has been removed [36].

2. Insufficient Transport Layer Protection: In wireless communications, if there is no encryption during the communication, it is easy to eavesdrop on data traffic and sensitive data might be stolen, even though, the data sent by the first router or wireless hotspot may be encrypted. However, there is no guarantee that an entire communication will be secure from a malicious attacker. So end-to-end encryption should be applied during the connection between the client and the server.

3. Poor Authorisation and Authentication: Poor authorisation and authentication are major problems on both client and server side. There should be mechanisms that guarantee that collectors only have access to their data, and this can be done only authentication and access control mechanisms are in place on the client application.

4. Data Recovery: It is important to have a recovery mechanism in case collectors or even project administrators lose their encryption keys or passwords.

5. Process to Process Communication and Separation: The data captured in the form of GPS-coordinates, video clips, and pictures are not under the direct control of the application, which only gets a copy or a link to it, and it is therefore very difficult to secure it or make sure it is deleted from the phone's memory.

c) General Security Approaches for Mobile Devices

There are a number of security approaches that can be regularly applied to mobile devices in order to manage their security. Some of them are:

1. General policy: An organisation should define the security policy regarding which types of the organisation's resources may be assessed via mobile devices and which types of mobile devices can be accessed via the organisation's information technology system. In the event that organisations allow their own employees to use personally-owned devices (Bring Your Own Device), they will need to have an appropriate policy in place. The centralized technology policy should enforce security on mobile devices. Some policies include managing the wireless network interface, how the organisation's system is administered, restricting user and application access to hardware, or automatically monitoring, detecting, and reporting when policy violations occur [37].

2.Data Communication and Storage: Encryption is a technique used for protecting the confidentiality of data. Strongly encrypted data communications are recommended to be applied between mobile devices and organisations. To prevent potential eavesdroppers, end-to-end encryption (E2EE) should be used in the process of data communications. The encryption should apply on both built-in mobile storage and removable mobile storage. Moreover, mobile devices should be configured to wipe themselves after a certain number of incorrect authentication attempts [37].

3. User and Device Authentication: Password-based authentication is a simple and popular technique for controlling access to data in mHealth systems. However, during a critical medical situation, the owners of a healthcare record may be unconscious and unable to provide the password in order to access their own healthcare records [38]. For this reason, biometrics are another possible solution for regulating access to healthcare records as they are physical attributes which stay with the owner at all times. User

Authentication is another solution to maintaining confidentiality of healthcare data which is stored in mobile devices. In general, automated authentication mechanisms can be broken down into three categories:

- **Something the user knows** (e.g. password, Personal Identification Number (PIN), pass phrase): This is the most common authentication method used for system users. Sometimes, the system may require a minimum length or special characters for the password in order to minimise the risk of guessing the correct password. As a result, something that the user knows can become something the user forgets.
- **Something the user possesses** (e.g. token, smart card): This authentication mechanism can replace the problem of forgetting a PIN or password. However, the user must carry this object with him/her at all times in order to gain access to mobile devices. Moreover, such anobject might be lost or stolen or can fall into the possession of an attacker [39].
- **Something the user is** (e.g. fingerprint, retina scan, voice print): This authentication mechanism is based on something intrinsic, also known as biometrics. Biometrics describes a physical feature unique to a person which can therefore be used to identify that person [40]. The main advantage of using biometrics in authentication mechanisms is that the user will always have the biometric component. In mHealth systems, voice printing and facial recognition have the most potential because of current audio and visual recording standards on many of the latest mobile devices [41]. However, biometric sensors are quite expensive and sometimes inaccurate. See the comparison of different type of biometrics in Table 3:

Type of Biometrics	Security Level	Cost	Size of Device
Fingerprint Recognition	Medium	Low	Small
Finger Vein Pattern	High	Medium	Small to Medium
Palm Vein Pattern	High	Medium	Medium
Facial Recognition	Low	Medium	Medium to Large
Iris Recognition	High	Medium to High	Large

Table 3: The Comparison of Biometrics [40]

The authentication mechanisms that have been mentioned above may provide some security level for mHealth devices. Therefore, the Multi-Factor Authentication, which is strong encryption that meets at least two requirements of something the user knows, something the user possesses, and something the user is [41], should be introduced as another solution to mHealth systems in order to increase the security of the authentication mechanism.

4. Applications: This includes restrictions regarding which applications may be installed on the device, restricting the permissions (e.g. location service, camera) assigned to each application, ensuring that applications have been installed and updated properly, and verifying digital signatures on applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified.

2) Managing mHealth data in Cloud Computing

There are four primary cloud deployment models. They represent the different categories of the cloud environment and are mainly distinguished by proprietorship, size, and access. The four types of cloud deployment model are:

- *Private Cloud:* The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.
- *Community Cloud:* The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.
- *Public Cloud:* The cloud infrastructure is provisioned for open use by the general public.
- *Hybrid Cloud:* The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public).

Occasionally, the cloud deployment model will be dictated by the type of application moving to the cloud. Initially, cloud deployments for clinical applications will take root in private or hybrid clouds given that these applications require the highest level of security, privacy, and availability. Non-clinical applications are a better fit for public deployment models but still must be carefully assessed [42].

a) Challenges in Managing Data in Cloud Computing

The cloud environment provides a new set of challenges including:

- Without a Service Layer Agreement (SLA) to limit the movement of data in cloud infrastructure, data can be anywhere in the cloud.
- Data can be moved from one location to one another (not static).
- The cloud provider might replicate data for legitimate reasons.
- The cloud provider administration needs access to the data block on the physical device.
- Because of cloud user virtualization, if data has been tampered with, it is very difficult to discover how and when such tampering occurred.
- Mobile services mean that services are now mobile, so it is difficult to track what the services do with data.
- Therefore, it is difficult to discover data breaches using the cloud.

b) Cloud Security Frameworks and Requirements

In public cloud storage systems, computing resources are shared among the cloud's users. Therefore, users may lose control over physical security with the utilization of the cloud. In this section some existing studies in security frameworks and requirements are discussed.

1. A detailed specification was developed by Firesmith [9]. It attempts to provide a comprehensive security framework which can be defined as follows:

- *Access Control:* The degree to which the system limits access to its resources only to its authorised externals.
- *Attack/Harm Detection:* The degree to which attempted or successful attacks are detected, recorded and notified.
- *Integrity:* The degree to which components are protected from intentional and unauthorised corruption.

- *Non-repudiation:* The degree to which a party to an interaction is prevented from successfully repudiating any aspect of the interaction.
- *Privacy:* The degree to which unauthorised parties are prevented from obtaining sensitive information.
- *Security Auditing:* The degree to which security personnel are enabled to audit the status and use of security mechanisms by analyzing security related events.
- *Physical Protection:* The degree to which the system protects itself and its components from physical attack.

Every application, including those in mHealth systems, at the highest level of abstraction will tend to have the same basic kinds of valuable and potentially vulnerable assets. In mHealth systems, assets include healthcare information, mHealth devices, and cloud storage. Likewise, these assets are vulnerable to the same basic kinds of security threats from attacks by the same basic kinds of attackers who can be profiled with motivations and their typical levels of expertise and tools.

Firesmith also proposed the "Reusable Security Requirements Templates" as it can be argued that highly reusable requirements templates can be produced for reuse across most application domains including mHealth. The Reusable Security Requirements Templates can be defined as Requirements, Security Subfactors, Quality Measures, and Quality Criteria [9].

Unlike typical functional requirements, security requirements can potentially be highly reusable, especially if specified as instances of reusable templates [9]. Although, this security framework has not been directly implemented in either the context of mHealth or cloud computing, it provides a detailed overview of the security requirements for any secure information system [21]. However, this framework can be extended in order to develop a new information security framework for mHealth systems.

2. A comprehensive SecureCloud framework was proposed by Ahn, Joshi, and Takabi [10]. These authors proposed a comprehensive security framework for cloud computing environments which deals with issues such as identity management, access control, policy integration among multiple clouds, trust management between different clouds and between a cloud and its users, secure service composition and integration, and semantic heterogeneity among policies from different clouds. This framework ensures that only authorized users will be granted access to the stored data. The main focus on this security framework is to understand data protection and resources from a security breach in a cloud that provides shared platforms and services.

The key components of the cloud computing environment include *Service Integrator* and the *Security Management Component*. Service Integrator has components that are responsible for the establishment and maintenance of trust between the local provider domains and between the providers and the users. The security management component provides the security and privacy specification and enforcement functionality. The comprehensive SecureCloud framework consists of the six following modules:

- *Access Control Module:* This module is responsible for supporting providers' access control needs. Role Based Access Control (RBAC) has been introduced as a method used in the Access Control Module.
- *Policy Integration Module:* SAML, XACML, and WS standards are viable solutions that satisfy the need for a Specification framework to ensure that cross domain accesses are properly specified, verified, and enforced.
- *Service Management Module:* Responsible for secure service discovery, composition and provision but using an approach that also considers security and privacy issues.
- *Trust Management Module:* Responsible for negotiation, establishment and evolution in the overall system.
- *Heterogeneity Management Module:* Responsible for providing a global ontology and supporting semantic heterogeneity concerns related to policies.

Authentication and Identity Management Module: Responsible for authenticating users and services based on credentials and characteristics

3. Cloud Security Framework (CSF) was suggested by Brock and Goscinski [11]. In order to develop the Cloud Security Framework (CSF), Brock and Goscinski characterised the security problems of clouds, evaluated the security of current cloud environments and presented current security countermeasures. The main focus of this security framework is on cloud infrastructure protection, communication and storage security, authentication, and authorisation.

The Cloud Security Framework (CSF) is influenced by the Information Flow Control Model and Kerberos. There are two main components in CSF; a Gateway Server (GS) and a Single Sign-on Access Token (SSAT). GSs are located in the clouds and manage the security of those clouds in which they are located. A SSAT is one-time token that is a time-limited, non-forgeable and non-transferable entity, which is granted to cloud users. This token identifies the user, services that user wishes to use, and also provides verification tokens to prove the SSAT itself is valid. Only authorised users are allowed to use the token. Moreover, the token cannot be reused once it expires.

In terms of functionality, the CSF, therefore is similar to the Information Flow Control model which uses trusted capabilities and some elements from Kerberos. The CSF framework aims to use time-based access to grant authorised users access to the cloud, protects against forgery of authorisation and grants access to services in remote clouds on behalf of users.

4. In [12], Zissis and Lekkas examined user-specific security requirements for end clients. They proposed a security solution to a number of challenges in a cloud environment, including Confidentiality and Privacy, Integrity, and Availability, by using a trusted Third Party. The authors proposed a Trusted Third Party (TTP) service as a solution to providing end-to-end security services in the cloud environment. Trusted Third Party services will lead to the establishment of the necessary Trust level and provide ideal solutions to preserve the confidentiality, integrity, and authenticity of data and communications. Moreover, TTP is an ideal security facilitator in a cloud environment where entities belonging to separate administrative domains, with no prior knowledge of each other, require the establishing of secure interactions.

In a cloud environment, the users are required to use their own digital certificates (sometimes called SSL certificates), as a reliable passport, to authenticate themselves to a cloud service provider in order to validate their access rights to the cloud resources. This certificate is used in combination with

the service provider's certificate to create a secure SSL connection between them, thus encrypting exchanged data and assuring their security through the cloud infrastructure. The application providers are required to use their own digital certificates to authenticate themselves when communicating with the cloud as well as encrypting and decrypting application data. The proposed solution makes use of a combination of Public Key Cryptography, Single-Sign-On technology and Lightweight Directory Access Protocol (LDAP) to securely identify and authenticate implicated entities in a cloud environment system.

5. A security framework based on *Capabilities* was proposed by Mapp et al [13]. A capability is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use capabilities to access objects. A capability is defined to be a protected object which, by virtue of its possession by a user process, grants that process the right to interact with an object in certain ways. The capability logically consists of a reference that uniquely identifies a particular object and a set of one or more of these rights. In this framework, everything in the system including users, devices and patient data must be represented by a capability. Capabilities therefore need to be carefully managed and need to be protected against being created or changed in an inappropriate manner [13]. The security framework defines five layers including user, application, hypervisor, transport and storage, and the method that happens in each layer. As seen in Figure 7 below:

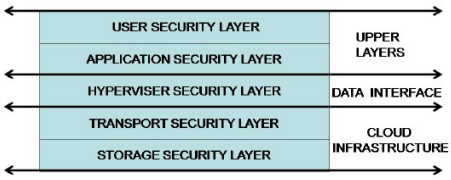

Figure 7: Security framework based on Capabilities [13]

- *User Security Layer:* In this layer, the cloud users will authenticate themselves to local device and application. This authentication will enable authorization to grant access to authorized users in order to access application resources.
- *Application Security:* This layer is used to authenticate the application to the hypervisor as well as responsible for Presentation Security which encodes and decodes data between the application and the Cloud Storage System.
- *Hypervisor Security Layer:* This layer is used to authenticate the application and user security layers to the Cloud Infrastructure and also used to generate capabilities which allow applications to access the required resources in the Cloud Infrastructure.
- *Transport Security Layer:* This layer provides the security of moving data between the application and the Cloud Infrastructure by using the Simple Protocol (SP) [13] which is a mechanism that provides quick authentication using key exchange.
- *Storage Security Layer:* This block uses encryption techniques including Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms to secure blocks of data in the Cloud Infrastructure.

However, this security framework does not specify security requirements for cloud storage in general. This is because this framework has been derived from the Firesmith framework [9] and looks at the functions of different parts of the cloud system in order to provide secure cloud storage.

Research by Yahya, Walters, and Wills [25] aimed to develop an appropriate security framework for cloud storage, which is the main component of mHealth systems, by exploring existing proposed security frameworks. The result from this research will identify which security requirements can be used as baselines to protect data in cloud storage. Security requirements mentioned in this research include Confidentiality, Integrity, Availability, Non-repudiation, Authenticity, and Reliability. According to interview results, all security experts commented that all proposed security requirements are important. However, Confidentiality, Integrity, and Availability are the most basic and common security requirements to form any security frameworks. Therefore, there is a need for a security framework that supports non-repudiation, accountability, and auditability (in order to be able to enable forensic analysis) which are also important security requirements in security systems. As a result, this is becoming the driving force behind the development of a new information security framework that support those necessary security requirements (i.e. non-repudiation, accountability, auditability) those are still missing from previous proposed security frameworks. Table 2 shows the comparison of different cloud security frameworks.

Security Requirement	**Author**				
	Firesmith [9]	Takabi, Joshi & Ahn [10]	Brock & Goscinski [11]	Zissis & Lekkas [12]	Mapp et al. [13]
Confidentiality	x	x	x	x	x
Integrity	x	x	x	x	x
Availability	x	x	x	x	x
Non-repudiation	x				
Authenticity			x	x	x
Reliability			x	x	x

Table 2: Synthesis of Security Requirements [25]

From the previous studies, several information security frameworks for mHealth devices as well as information security frameworks for cloud storage have been proposed. However, a major challenge is developing an effective information security framework that will encompass both mHealth devices and cloud storage in order to protect the confidentiality of healthcare data in mHealth systems.

3. KEY MECHANISMS FOR PROVIDING POSSIBLE SOLUTIONS TO MANAGE MHEALTH DATA

As part of investigating the development of a new security framework, based on the previous work of Mapp et al. [13], there are some possible solutions for managing mHealth data using various techniques/mechanisms. These mechanisms will be able to deliver the security components as part of an mHealth Taxonomy. The mechanismsare identified as follows:

1.) **Encryption as a Service:** This mechanism will apply to healthcare data which is the second domain of the mHealth taxonomy. All healthcare data in the mHealth system should be stored and transported in an encrypted fashion to protect the confidentiality of data at all levels of an mHealth system. There is the need for encryption except during the time that the data is actually being used for a given task. Only the application that owns or has been given access by the user is allowed to decrypt the data. It also needs to be able to guarantee personalized access.

The main purpose of encryption is to provide the confidentiality of data that is stored in mHealth systems. However, encryption does not prevent communication interception nor guarantee end-to-end confidentiality [26]. It is true that the interceptor will only be able to access the ciphertext but cannot decrypt it. However, there are times when the plaintext itself may be stored in vulnerable places not protected by the encryption process. Moreover, encryption itself provides only confidentiality of data but does not provide other security requirements such as integrity, authenticity, or non-repudiation but it can be used to help provide other security services. For example, Encryption can be used to design a Message Authentication Code (MAC) which provides data origin authentication [26]. Therefore, other security mechanisms may be required in mHealth systems in order to protect healthcare data elsewhere in the mHealth system.

2.) **Capabilities:** Capability based authorization is a concept in the design of secure cloud computing systems (one of the existing security models). Capabilities therefore need to be carefully managed and need to be protected against being created or changed in an inappropriate manner [13]. Because of the large quantities of data to be managed, capabilities are now being used to secure objects compared to using Access Control Lists (ACLs).

To develop Capabilities as a solution for managing mHealth data, Internet Protocol version 6 (IPv6) addresses can be modified in order to support a Capability-ID system. IPv6 is the most recent version of the Internet Protocol (IP). IPv6 is a 128 bit communication protocol that provides an identification and location system for computers on networks across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) with the intention of replacing IPv4 [35]. However, the improvements of IPv6 have not been able to be fully used in mobile and cloud system environments. Therefore, IPv6 should be modified in order to give more support to mHealth systems [13].

3.) **Storage Management**: This mechanism provides the management of security for each block of data in the cloud infrastructure using encryption techniques such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard) algorithms to provide the confidentiality of data. Moreover, each block of data is hashed after it has been modified in order to provide integrity so that data will not be able to modified by an unauthorized user. In order to ensure the availability of data, each block may be replicated throughout the cloud storage structure. Therefore, a coherency protocol within the storage layer is used to synchronize different copies of the block [13].

4.) **Digital Filter:** In addition to traditional security measures, the use of digital filters should be an additional advantage in providing more control on persons who are enabled to access healthcare data. Each healthcare record in an mHealth database can have a set of filters which are used to prevent certain fields in that record from being accessed. In order to access a given field, the relevant filter must be removed. This usually requires authorisation from senior personnel. This will also enable the tracking of how the data is used.

5.) **Secure Transport:** Confidentiality is a key part of information services and it should be dealt with at the Transport Services level. An examination of network interactions at the local area level clearly indicates that there is a need for much more transactional support in the cloud environment as there is a large amount of client/server interaction in order to use network services [13]. As a result, the Simple Protocol (SP) [43] has been developed to deal with this issue. Unlike Transmission Control Protocol (TCP) which is a stream-based message protocol, messages in SP will be divided into blocks before transmission over the network interface [44]. The advantage of SP is that it provides a reliable service and can run over unreliable data substrates such as a User Datagram Protocol (UDP) or raw Ethernet [13].

SP is very lightweight and therefore can be combined with Encryption as a Service to provide secure communications while maintaining fast connections.

6.) **Blockchain:** Nowadays, blockchains (or sometimes called distributed ledger technology) are being used to provide a more secure Internet (IPFS as a replacement for http) [45]. The blockchain is a distributed data system where users share a consistent copy of a database and agree on changes by consensus. The data is composed in form of blocks, where each block includes a cryptographic signature of the previous block, creating an immutable record [46]. The users must comply with ledger rules including Permissionless ledger (anyone could join), and Permissioned ledger (participation is subject to rules of the members). The blockchain uses a type of consensus protocol in order to agree on the validity of a given transaction. It also uses digital signatures (private/public key) to sign and/or encrypt transactions on the ledger by which each signature could be linked to identity of the owner [47]. The blockchain provides an advantage to a distributed network of computers that do not necessarily trust each other to achieve consensus [48]. Moreover, the blockchain is the technology that supports security requirements that were missing from previously proposed information security frameworks [25] which include non-repudiation, accountability, and auditability.

7.) **Secure Transactional Layer:** Secure Remote Procedure Call (RPC) protects the remote procedure by applying an authentication mechanism. Secure RPC provides servers with the validated identity of remote users which servers can then use for access control. The identity of the user is guaranteed by secure RPC through the use of encryption [49]. A strongly typed RPC will be implemented at the Secure Transactional Layer so that both nature of parameters as well as value are transferred between client and server. Hence, this mechanism can prevent immersing attacks such as buffer attack on the web server.

8.) **Service Management Platform:** The service management platform deals with how services are registered in a cloud which also includes the overall service and Security Level Agreement (SSLA) between the service providers and the cloud providers as well as stores the record of unique service ID that has been assigned to each service [50].

4. DEVELOPING THE NEW SECURITY FRAMEWORK

In this section, the new security framework for the cloud-based infrastructure in Figure 8is proposed based on the use of key mechanisms from Section 3. Cloud storage plays a big role in mHealth systems. Healthcare data that has been collected from mHealth devices will be transmitted over the network and mainly stored in cloud storage. Therefore, it is necessary to develop the security framework that will be able to provide a complete set of security requirements for components present in the mHealth system taxonomy.

APPLICATIONS
APPLICATION DEVELOPMENT LAYER
SERVICE MANAGEMENT PLATFORM
SECURE TRANSACTIONAL LAYER
BLOCKCHAIN SYSTEM
TRANSPORT SECURITY LAYER
DIGITAL FILTER SYSTEM
STORAGE MANAGEMENT LAYER
CAPABILITY SYSTEM
OS LAYER

Figure 8: The new security framework

The new security is described below in the context of Figure 8. Healthcare data in mHealth systems, will be stored in the form of blocks using a *Blockchain* mechanism. Each block of data will be encrypted with the strongest algorithm and is stored separately in the cloud storage. Every objectin a mHealth system (such as users of mHealth devices, healthcare professionals, mHealth devices, healthcare data)will be managed using *Capabilities.* This is in order to organize access rights which can ensure that only authorized personal will be able to access healthcare data stored in the cloud. To deliver additional control by which users will be able to access healthcare data, *Digital Filters* will be applied to healthcare data to prevent certain fields of data from being accessed by unrelated stakeholders. The *Service Management Platform* will define the requirement to run the service to a level that the cloud provider considers adequate. In order to achieve this requirement, each service must provide a list of parameters which must be agreed with those parameters obtained by the cloud. This parameter list is also used to migrate the service in order to find appropriate clouds that can accept the service [50]. The *Secure Transactional Layer* will secure the remote procedure between stakeholders and cloud server by applying an authentication mechanism. The *Transport Security Layer* will use the Simple Protocol (SP), which is the security mechanism that provides the authentication by using key exchange, in order to secure the transmission of healthcare data between stakeholders and the cloud infrastructure. Furthermore, The *Storage Management Layer* will apply encryption techniques, and hash and replicate each block of healthcare data to provide confidentiality, integrity and availability of data.

5. AN ADVANCED DIGITAL MEDICAL PLATFORM

The new Security Framework for mHealth can be used to develop an Advanced Medical Digital Platform (ADIMEP) as shown in Figure 9. The system uses a Capability Management Unit (CMU) to manage the front-end of the ADIMEP, which is concerned with the medical devices, that are used to take readings at home or carried by the user. The CMU also manages access to patient records by healthcare professional as well as patient monitoring and appointment routines.

The back-end uses the Storage Management System to provide persistent storage of objects. The Storage Management System can be broken down into an object management, file management and cloud-block management subsystems.

Finally, the research end allows medical researchers to have access to medical data in real-time, without the need to generate costly modified data sets because digital filters will allow the data needed by the researchers to be available while not allowing access to more sensitive personal data. So through this new framework, an ADIMEP can be used to address in scenario described in Section 2.

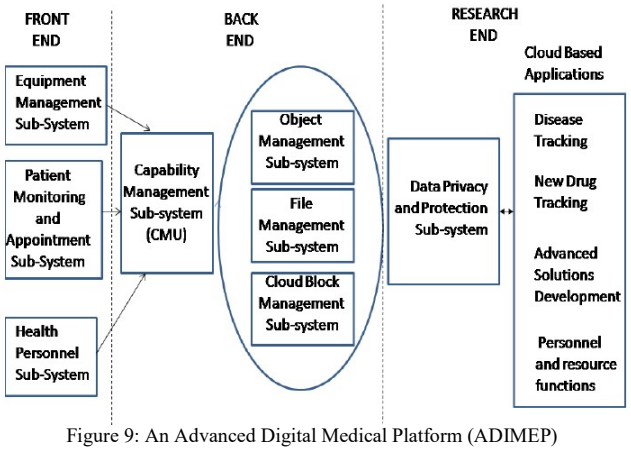

Figure 9: An Advanced Digital Medical Platform (ADIMEP)

6. FUTURE WORK

An mHealth ontology will be developed from the mHealth taxonomy given in this work by defining attributes and relationships between entities, as well as classes of things that are characterized by these attributes and relationships [51].

In mHealth systems, data could be generated from many different sources. As a result, the amount and diversity of data could further complicate the matter. Hence, it is necessary to apply security mechanisms to protect the security of data at every level. Developing an ontology will give some benefits in correlating security data coming from different sources, and also systematically capturing and properly representing the system in the way that will be understood not only just by technical staff but also general users.

Some reasons to develop and use an ontology in an mHealth system are also presented below [52][53]:

- *To share common understanding of the structure of information among general users and software agents*- The development of ontologies creates a conceptual model that makes it possible to better understand its domain.
- *To enable reuse of domain knowledge* – The developed ontologies could be simply reused for their domains, or extended to describe different domains of interest.
- *To make domain assumptions explicit* – Underlying an implementation makes it possible to change these assumptions easily if knowledge about the domain changes.

- *To enable knowledge sharing* – The ontology can become extremely valuable for those who have similar needs for knowledge representation on the ontology domain.
- *To cover the whole range of security needs* – There are many security tools have been developed to tackle various vulnerabilities that exist in the system. However, each tool was designed to detect only specific attacks; none of them ensure the whole range of security needs. Systematically mapping the system using an ontology will generate a format that can be easily understood to develop security mechanisms which will be applied at all levels of the system.

In an mHealth system, the ontology can be used to systematically map the state of research and practice in mHealth, discover gaps in research and between research and practice, and also formulate a strategy to bridge these gaps. The ontological map can be used to illuminate the big picture of the domain of an mHealth system.

Moreover, the new information security framework presented in Section 4 could be developed and implemented in order to build a prototype version of ADIMEP.

7. SUMMARY AND CONCLUSIONS

Nowadays, mHealth technology provides new opportunities to deliver healthcare service to users anywhere and at any time through the use of mobile devices and applications. Managing mHealth data has become a major issue in mHealth. Cloud computing is a relatively new type of information technology which provides more efficient processing and data storage with less expense to end users in the healthcare service. However, there are still many challenges related to the process of transferring and storing healthcare data in both of mHealth devices and cloud storage. Perhaps the most important of these challenges is ensuring the security of data.

This paper has focused on developing a new information security for mHealth to meet the challenges of this new environment. It examined previous information security frameworks for both mHealth devices and cloud storage systems. It then performed a detailed domain analysis and identified the additional need to provide mechanisms to support non-repudiation, accountability and auditability. Finally it highlighted key mechanisms that could be used to build this new and comprehensive information security framework for mHealth. Going forward, this work will allow us to design a detailed ontology for a secure mHealth system and to build a prototype environment as part of an Advanced Digital Medical Platform (ADIMEP).

REFERENCES

1. World Health Organisation (2011) *mHealth: New horizons for health through mobile technologies.* [online]Available from: http://www.who.int/goe/publications/goe_mhealth_web.pdf [Accessed: 6 January 2017]
2. European Commission (2014) *GREEN PAPER on mobile Health ("mHealth").* [online] Available from: https://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth [Accessed: 10 January 2017]
3. Germanakos P., Mourlas C., & Samaras G. "A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems" Proceedings of the Workshop on *'Personalization for e-Health' of the 10th International Conference on User Modeling (UM'05)*. Edinburgh, July 29, 2005, pp. 67–70.
4. European Commission (2014) *Healthcare in your pocket: unlocking the potential of mHealth.* [online] Available from: http://europa.eu/rapid/press-release_IP-14-394_en.htm [Accessed: 10 January 2017]
5. Whittaker, R. (2012) *Issues in mHealth: Finding From Key Informant Interviews.* [online] Available from: http://www.jmir.org/2012/5/e129/ [Accessed: 10 January 2017]
6. Avancha, S., Baxi, A. & Kotz, D. (2012) *Privacy in mobile technology for personal healthcare.* ACM Comput. Surv. 45, 1, Article 2 (November 2012), 54 pages.
7. Vodafone Global Enterprise (2013) *Evaluating mHealth Barriers: Privacy and Regulation.* [online] Available from: http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-EvaluatingmHealth-Adoption-Privacy-and-Regulation.pdf [Accessed: 20 January 2017]
8. Adesina, A.O., Agbele, K.K., Februarie, R., Abidoye, A.P., Nyongesa, H.O. (2011) *Ensuring the security and privacy of information in mobile health-care communication systems.* S Afr J Sci. 2011;107(9/10), Art. #508, 7 pages. Doi:10.4102/sajs.v107i9/10.508
9. Firesmith, D. "Specifying Reusable Security Requirements" Journal of Object Technology. Vol.3, no.1, pp.61-75, 2004.
10. Takabi, H., Joshi, J.B.D., & Ahn, G.J. "SecureCloud: Towards a comprehensive security framework for cloud computing environments". International Computer Software and Applications Conference, 2010, pp.393-398.
11. M. Brock, and A. Goscinski, A."Toward a Framework for Cloud Security" in Lecture Notes in Computer Science, vol 6082, Springer Berlin Heidelberg, 2010, pp.254-263.
12. Zissis, D. and Lekkas, D. "Addressing cloud computing security issues". Future Generations Computer Systems. 28(2012). P.583-592.
13. Mapp, G., Aiash, M., Ondiege, B., & Clarke, M (2014) Exploring a New Security Framework for Cloud Storage Using Capabilities. *In: 2014 IEEE 8th Symposium on Service Oriented System Engineering (SOSE).* Oxford: IEEE, P. 484-489
14. Hunter, A. (N/A) *Taxonomies* [online] Available from: http://www0.cs.ucl.ac.uk/staff/a.hunter/tradepress/tax.html [Accessed: 25 January 2017]
15. Noy. N. F, & McGuinness, D. L. (2001) *Ontology Development 101: A Guide to Creating Your First Ontology* [online] Available from: http://protege.stanford.edu/publications/ontology_development/ ontology101.pdf [Accessed: 19 January 2017]
16. Gonzalez, N.M., Miers, C.C., Redigolo, F.F., Simplicio, M., Carvalho, T., Naslund, M., & Pourzandi, M. (2011) A Taxonomy Model for Cloud Computing Services. *In: 1st International Conference on Cloud*

Computing and Services Science (CLOSER). Netherlands: Springer, pp.56-65.

17. Mell, P., and Grance, T. The NIST definition of cloud computing. Commun ACM 2010;53(6):50.
18. Johnston, S. (2008) Taxonomy: The 6 layer Cloud Computing Stack [online] Available from: https://samj.net/2008/09/17/taxonomy-the-6-layer-cloud-computing-stack/ [Accessed: 16 March 2017]
19. U.S. Food & Drug Administration (2015) *Implants and Prosthetics* [online] Available from: http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ImplantsandProsthetics/ [Accessed: 10 January 2017]
20. Medical Device and Diagnostic Industry (2013) *Body Hackers Implant Homemade Health Monitor* [online] Available from: http://www.mddionline.com/blog/devicetalk/body-hackers-implant-homemade-health-monitor [Accessed: 10 January 2017]
21. Karulf, E. (2008) Body Area Networks (BAN) [online] Available from: http://www.cse.wustl.edu/~jain/cse574-08/ftp/ban/index.html [Accessed: 10 January 2017]
22. Jovanov, E. (2005) Wireless technology and system integration in body area networks for m-health applications. In: *2005 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Science (EMBS).* Shanghai: IEEE, pp. 7158-7160
23. HealthIT.gov (2016) *Are there different types of personal health records (PHRs)?* [online] Available from: https://www.healthit.gov/providers-professionals/faqs/are-there-different-types-personal-health-records-phrs [Accessed: 11 January 2017]
24. Dumortier, J and Verhenneman, G. (2013). *Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the US* in Carlisle George, Diane Whitehouse and Penny Duquenoy (eds). eHealth: Legal, Ethical and Governance Challenges, Springer-Verlag.
25. Yahya, F., Walters, R.J., & Wills, G.B. (2016) Goal-Based Security Components for Cloud Storage Security Framework: A Preliminary Study. *In: 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).* London: IEEE, P.1-5
26. Martin, K. (2012) *Everyday Cryptography.* United States of America: Oxford University Press Inc.
27. Kang, J, & Adibi, S. (2015) A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN). "*The series of Communications in Computer and Information Science"*, Volume 523, P.61-83.
28. Convery, S. (2007) Network Authentication, Authorization, and Accounting, *"The Internet Protocol Journal"*, Volume 10, pp.2-11.
29. International Organization for Standardization (2011) *ISO27005:2011Information Security-- Security Techniques – Information Security Risk Management* [online] Available from: https://www.iso.org/standard/56742.html [Accessed: 17 March 2017]
30. El-Abed, M., Giot, R., Hemery, B., Schwartzmann, J, & Rosenberger, C. (2012) Towards the Security Evaluation of Biometric Authentication Systems. *IACSIT International Journal of Engineering and Technology*. 4(3), pp.315-320.
31. CSA (2016) The Treacherous 12 Cloud Computing Top Threats in 2016 [online] Available from: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf [Accessed: 17 March 2017]
32. Savage, M. (2012) *Mobile device protection: Tackling mobile device security risks.* [online] Available from: http://searchsecurity.techtarget.com/magazineContent/Mobile-device-protection-Tackling-mobile-device-security-risks [Accessed: 15 January 2017]
33. Gejibo, S., Mancini, F., Mughal, K.A., Valvik, R.A., & Klungsoyr, J. (2012) Secure Data Storage for Java ME-Based Mobile Data Collection Systems. In: *2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom 2012).* Beijing: IEEE, P.498-501.
34. Jung, C. (2011) *Mobile Data Collection Systems: A review of the current state of the field.* [online] Available from: https://humanitarian-nomad.org/wp-content/uploads/2013/03/NOMAD-MDC-Research.pdf (Accessed: January 18th, 2017).
35. Gejibo, S.H. (2015) *Towards a Secure Framework for mHealth.* PhD. University of Bergen.
36. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W. Calandrino, J.A., Feldman, A.J., Appelbaum, J., & Felten, E.W. (2008) Lest We Remember: Cold Boot Attack on Encryption Keys. *In: Proc. 17th USENIX Security Symposium (Sec'08)*, San Jose, CA.
37. Scarfone, K.&Souppaya, M. (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. [online] Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [Accessed: 15 January 2017]
38. Gardner, R.W., Garera, S., Pagano, M.W., Green, M., & Rubin, A.D. (2009) Securing Medical Records on Smart Phones. In: *2009 16th ACM Conference on Computer and Communications Security (CCS).* Chicago: ACM, pp.31-40.
39. Schneider, F.B. (N/A) *Something You Know, Have, or Are* [online] Available from: https://www.cs.cornell.edu/courses/cs513/2005fa/NNLauthPeople.html [Accessed: 18 January 2017]
40. ICD Security Solutions (2012) *Access Control Continued: biometrics and other forms of access authorization* [online] Available from: https://www.icdsecurity.com/2014/10/20/access-control-continued-biometrics-and-other-forms-of-access-authorization/ [Accessed: 18 January 2017]
41. Luxton, D.D., Kayl, R.A., & Mishkind, M.C. (2012) mHealth Data Security: The Need for HIPAA Compliant Standardization. *In: Telemedicine & e-Health*, Volume 18, Issue 4, P.284.
42. Cloud Standards Customer Council (2012) Impact of Cloud Computing on Healthcare. [online] Available from: http://www.cloud-

council.org/deliverables/CSCC-Impact-of-Cloud-Computing-on-Healthcare.pdf [Accessed: 18 January 2017]
43. Mapp, G., & Riley, L. (2014) *yRFC3: The Simple Protocol Lite (SP-Lite) Specification* [online] Available from: http://www.mdx.ac.uk/__data/assets/pdf_file/0030/124797/yrfc3-SP-Lite.pdf [Accessed: 20 January 2017]
44. Padiy, A.& Mapp, G. (N/A) *Simple Protocol - Java userspace implementation* [online] Available from: http://www.mdx.ac.uk/__data/assets/pdf_file/0019/50059/Simple-Protocol-Java-Userspace-Implementation.pdf [Accessed: 22 January 2017]
45. TayloyWessing (N/A) *How secure is blockchain?* [online] Available from: https://www.taylorwessing.com/download/article-how-secure-is-block-chain.html [Accessed: 23 January 2017]
46. Korolov, M. (2016) *The blockchain is now being hyped as the solution to all inefficient information processing systems* [online] Available from: http://www.csoonline.com/article/3050557/security/is-the-blockchain-good-for-security.html [Accessed: 23 January 2017]
47. ENISA (2017) *Distributed Ledger Technology & Cyber Security – Improving information security in the financial sector* [online] Available from: https://www.enisa.europa.eu/publications/blockchain-security [Accessed: 25 January 2017]
48. Pair, S. (2015) *The Secure Blockchain is Bitcoin's Biggest Asset* [online] Available from: https://www.infosecurity-magazine.com/opinions/the-secure-Blockchain-is-bitcoins/ [Accessed: 23 January 2017]
49. Hall, M. & Barry, J. (2013) *The Sun Technology Papers.* The United States of America: Springer.
50. Sardis, F., Mapp, G., Loo, J., Aiash, M. & Vinel, A. (2013) On the Investigation of Cloud-based Mobile Media Environments with Service-Populating and QoS-aware Mechanisms. *In IEEE Transactions on Multimedia*. 15(4), pp.769-777.
51. TopQuadrant (2013) *Controlled vocabularies, taxonomies, and thesauruses (and ontologies)* [online] Available from: http://www.topquadrant.com/docs/whitepapers/cvtaxthes.pdf [Accessed: 25 January 2017]
52. Noy. N. F, & McGuinness, D. L. (2001) *Ontology Development 101: A Guide to Creating Your First Ontology* [online] Available from: http://protege.stanford.edu/publications/ontology_development/ ontology101.pdf [Accessed: 19 January 2017]
53. Moreira, E.S., Martimiano, L.A.F, Brandao, A.J.S, & Bernardes, M.C. (2008) Ontologies for information security management and governance. *Information Management & Computer Security*. 16(2), pp.150-165.